

1 **WO**

2
3
4
5
6 **IN THE UNITED STATES DISTRICT COURT**
7 **FOR THE DISTRICT OF ARIZONA**
8

9 Daniel Bozek, et al.,

10 Plaintiffs,

11 v.

12 Arizona Labor Force Incorporated, et al.,

13 Defendants.
14

No. CV-24-00210-PHX-SMB

ORDER

15 A group of hackers used ransomware to breach Defendant Arizona Labor Force
16 Inc.'s ("Labor Force") data system and to extract sensitive information of its employees.
17 Plaintiffs Daniel Bozek and Brandon Gaines (collectively, "Plaintiffs") filed this lawsuit
18 representing a proposed class of current and former employees (the "Proposed Class") who
19 had their data stolen (Doc. 16 (First Amended Class Action Complaint ("Amended
20 Complaint")))). Labor Force moves for judgment on the pleadings (Doc. 19). The parties
21 fully briefed the pending Motion (Doc. 20 (Plaintiffs' Opposition to Defendant's Motion
22 for Judgment on the Pleadings); Doc. 21 (Reply in Further Support of Motion for
23 Judgment on the Pleadings)). Labor Force requested oral argument (Doc. 19 at 1),
24 however, the Court will resolve the Motion without oral argument, finding it unnecessary.
25 *See* LRCiv. 7.2(f). Having reviewed the parties' briefs and the applicable law, the Court
26 will grant in part Labor Force's Motion and deny it in part for the following reasons.

27 ///

28 ///

1 **I. BACKGROUND**

2 For purposes of the pending Motion, the Court derives the following facts from
3 Plaintiffs' Amended Complaint. (*See* Doc. 16 ("Amended Compl.".)

4 Labor Force operates a nation-wide staffing agency. Labor Force collects and
5 maintains its employees' data electronically on its systems. Around January 9, 2023, a
6 ransomware group attacked Labor Forces' data system, stealing its current and former
7 employees' sensitive data. The stolen data included employees' personally identifiable
8 information ("PII") like names, addresses, social security numbers, and tax information
9 (collectively, "sensitive information"), and wound up on the dark web for sale where
10 unauthorized individuals had unfettered access. Labor Force did not notify the employees
11 nor a state attorney general about the breach.

12 Plaintiffs allege that Labor Force knew or should have known about the risk of
13 breaches and failed to adequately safeguard its system given the rise of breaches across the
14 nation in the past few years. And Labor Force was keenly aware of the sensitive nature of
15 their employees' data. Additionally, the failure to keep the data secure exposed the Class
16 to a robust cyber black market where their data can be purchased and used to commit
17 various crimes. Plaintiffs further allege that Labor Forced failed to comply with the Federal
18 Trade Commission's ("FTC") guidelines for data security or even take basic security
19 measures. Plaintiffs also allege that Labor Force failed to comply with industry standards
20 of proper encryption of PII, training employees on how to protect PII, and correct software
21 and network configurations.

22 As a result of its failure to safeguard the Class's data, implement appropriate
23 security measures, and protect against foreseeable threats, Plaintiffs allege to have suffered
24 damages caused by said failure. Those damages include: (1) compromise, publication, and
25 unauthorized use of their data; (2) expenses associated with preventing, detecting, and
26 recovering from identity theft or fraud; (3) lost opportunity costs from responding to
27 mitigating the effects of the breach; (4) continued risk to their sensitive information as it
28 remains in Labor Force's possession; and (5) current and future costs for time, effort, and

1 money expended to prevent, detect, contest, remedy, and repair the impact of the data
 2 breach. Plaintiffs assert claims for (1) negligence; (2) invasion of privacy; (3) breach of
 3 implied contract; (4) breach of fiduciary duty; (5) breach of confidence; (6) violation of the
 4 California Unfair Competition Law (“UCL”); (7) violation of the California Customer
 5 Records Act (“CRA”); and (8) violation of the California Consumer Privacy Act (“CPA”).

6 Labor Force now moves for judgement on the pleadings under Federal Rule of Civil
 7 Procedure 12(c). Labor Force contends that Plaintiff’s lack standing and have otherwise
 8 failed to state claims under any cause of action. (Doc. 19.)

9 **II. LEGAL STANDARD**

10 Under Federal Rule of Civil Procedure 12(c), “a party may move for judgment on
 11 the pleadings” after the pleadings are closed “but early enough not to delay trial.” A motion
 12 for judgment on the pleadings can be brought to challenge the legal sufficiency of the
 13 opposing party’s pleading. *Westlands Water Dist. v. United States*, 805 F. Supp. 1503,
 14 1506 (E.D. Cal. 1992). The motion should only be granted if “the moving party clearly
 15 establishes on the face of the pleadings that no material issue of fact remains to be resolved
 16 and that it is entitled to judgment as a matter of law.” *Hal Roach Studios, Inc. v. Richard*
 17 *Feiner & Co., Inc.*, 896 F.2d 1542, 1550 (9th Cir. 1989). Despite the difference in timing
 18 between the two motions, a Rule 12(c) motion is functionally identical to a Rule 12(b)(6)
 19 motion to dismiss for failure to state a claim, and the same legal standard applies to both
 20 motions. *Dworkin v. Hustler Magazine, Inc.*, 867 F.2d 1188, 1192 (9th Cir. 1989).

21 To survive a Rule 12(b)(6) motion for failure to state a claim, a complaint must meet
 22 the requirements of Rule 8(a)(2). Rule 8(a)(2) requires a “short and plain statement of the
 23 claim showing that the pleader is entitled to relief,” providing “fair notice of what
 24 the . . . claim is and the grounds upon which it rests.” *Bell Atl. Corp. v. Twombly*, 550 U.S.
 25 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). This exists if the
 26 pleader sets forth “factual content that allows the court to draw the reasonable inference
 27 that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662,
 28 678 (2009). Dismissal under Rule 12(b)(6) “can be based on the lack of a cognizable legal

theory or the absence of sufficient facts alleged under a cognizable legal theory.” *Balistreri v. Pacifica Police Dep’t*, 901 F.2d 696, 699 (9th Cir. 1988). A cognizable legal theory must state a claim to relief that is “plausible on its face.” *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). Plausibility does not equal “probability,” but requires “more than a sheer possibility that a defendant has acted unlawfully.” *Id.* The Court views the well-pled factual allegations as true and construes them in the light most favorable to the nonmoving party. *Cousins v. Lockyer*, 568 F.3d 1063, 1067 (9th Cir. 2009). But legal conclusions couched as factual allegations are not given a presumption of truthfulness, and “conclusory allegations of law and unwarranted inferences are not sufficient to defeat a motion to dismiss.” *Pareto v. FDIC*, 139 F.3d 696, 699 (9th Cir. 1998).

III. DISCUSSION

A. Article III Standing

Labor Force asserts a facial attack on Plaintiffs’ Article III standing based on allegations contained in the Amended Complaint. (*See* Doc. 19 at 10.) Under Federal Rule of Civil Procedure 12(b)(1), a defendant may challenge a plaintiff’s jurisdictional allegations using a “facial” attack, in which the allegations are accepted as true but that they are insufficient to invoke federal jurisdiction. *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014). The Court resolves a facial attack as it would a motion to dismiss under Rule 12(b)(6). *Id.* Before the Court may reach the merits of Plaintiffs’ claims, it must first determine if it has subject matter jurisdiction.

To bring a justiciable lawsuit into federal court, Article III of the Constitution requires that a plaintiff have “the core component of standing.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). To establish Article III standing, an injury must be “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013) (citation omitted). A “speculative chain of possibilities” cannot establish an actual or imminent injury in fact. *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 414 (2013); *see also FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 231 (1990) (“It is a long-settled principle

1 that standing cannot be ‘inferred argumentatively from averments in the pleadings,’ but
2 rather ‘must affirmatively appear in the record.’” (internal citations omitted)).

3 Labor Force’s standing challenge lies purely in the causation requirement, of which
4 it argues that Plaintiffs fail to adequately allege a connection between their injuries and the
5 data breach. (Doc. 19 at 11–12.) According to Labor Force, Plaintiffs’ allegations boil
6 down to conclusory allegations that Plaintiffs were once employed, the breach occurred,
7 and that their sensitive information is on the dark web, and as such the allegations are
8 factually deficient to support standing. (*Id.* (citing *Anderson v. Kimpton Hotel & Rest.*
9 *Grp.*, LLC, No. 19-CV-01860-MMC, 2019 WL 3753308 (N.D. Cal. Aug. 8, 2019); *Bass*
10 *v. Facebook, Inc.*, 394 F. Supp. 3d 1024 (N.D. Cal. 2019)); *see also* Doc. 21 at 6–8.) In
11 response, Plaintiffs argue they have adequately established causation because, in addition
12 to those facts, Labor Force failed use proper security protocols, failed to properly train its
13 employees, and left the data unencrypted. (Doc. 20 at 7–9.)

14 The cases Labor Force cites for support are unavailing and Labor Force fails to
15 address the facts alleged supporting the unreasonableness of their security measures that
16 render those cases distinguishable. In *Anderson*, the plaintiff asserted general allegations
17 that the defendant “failing to implement and maintain reasonable security procedures and
18 practices,” “fail[ed] to establish and implement appropriate . . . safeguards,” and “left [the
19 plaintiff’s] PII inadequately protected.” 2019 WL 3753308, at *4 (first alteration in
20 original) (“In particular, the complaint does not allege the nature of any assertedly
21 reasonable, appropriate, obligatory, sufficient and/or adequate action [the defendant] failed
22 to take.”).

23 In *Bass*, the plaintiff alleged that “(i) he had been forcibly logged out of his
24 Facebook account; (ii) he received phone calls from people purporting to be his family
25 members; and (iii) he subsequently received fake Facebook friend requests, spam e-mails,
26 and pornographic links on his Facebook messenger service.” 394 F. Supp. 3d at 1036. On
27 these facts, the court found traceability was lacking because there was no connection to the
28 breach and noted that Facebook, not the hackers, caused the log-out, the hackers did not

1 call the victims of the breach, and friend requests are common occurrences that do not
 2 establish a connection to the actual breach at issue. *Id.* (“[T]hat Facebook did not notify
 3 [the] plaintiff[] that he had been victimized by the data breach does not foreclose a plausible
 4 allegation at this early stage.”).

5 Plaintiffs allege that they: (1) took reasonable steps to maintain the confidentiality
 6 of their sensitive information; (2) their employment required disclosing the sensitive
 7 information; (3) Labor Force stored that data on their systems; (4) Labor Force failed to
 8 implement basic security safeguards to protect those systems, including “(a) the proper
 9 encryption of PII; (b) education and training employees on how to protect PII; and (c)
 10 correcting the configuration of software and network devices”; (5) hackers breached the
 11 systems; (6) Labor Force did not notify Plaintiffs of the breach; and (7) Plaintiffs learned
 12 after the breach that their sensitive information was available on the dark web “with
 13 indications that it came from [Labor Force’s] systems” exposing them to an increased risk
 14 of fraud and identity theft and costs associated with mitigating such risks. (Amended
 15 Compl. at 4 ¶¶ 14–16, 5 ¶ 24, 6 ¶¶ 27–29, 31, 8 ¶ 40, 10–11 ¶ 51, 14 ¶ 65, 18 ¶ 78.)

16 For standing purposes and accepting the allegations as true, the inclusion of these
 17 facts sufficiently distinguishes this case from *Anderson and Bass*. *See, e.g., In re Sequoia*
 18 *Benefits & Ins. Data Breach Litig.*, No. 22-CV-08217-RFL, 2024 WL 1091195, at *2 (N.D.
 19 Cal. Feb. 22, 2024) (finding similar allegations sufficiently established traceability); *Baton*
 20 *v. Ledger SAS*, No. 21-CV-02470-EMC, 2024 WL 3447511, at *13–14 (N.D. Cal. July 16,
 21 2024) (finding allegations that the defendant failed to implement adequate security
 22 measures and failed to notify the plaintiffs was sufficient to establish traceability);
 23 *Samantha Landon v. TSC Acquisition Corp.*, No. 2:23-CV-01377-SVW-PD, 2024 WL
 24 5317240, at *3 (C.D. Cal. Nov. 1, 2024) (finding traceability where plaintiff alleged her
 25 social security number was potentially stolen in a data breach and posted on the dark web).
 26 As alleged, these facts fall like dominos, layering on one another to create reasonable
 27 inferences that Plaintiffs’ sensitive information was posted to the dark web because it was
 28 stolen in the breach from Labor Force’s unreasonably unsecure systems and is thus fairly

traceable. *See, e.g., Wash. Env't Council v. Bellon*, 732 F.3d 1131, 1141–42 (9th Cir. 2013) (noting, for standing purposes, a “causal chain does not fail simply because it has several links, provided those links are not hypothetical or tenuous and remain plausible”). Accordingly, the Court declines to grant judgment on standing grounds.

B. Failure to State a Claim

Next, Labor Force argues that Plaintiffs fail to state a claim under all causes of action. (Doc. 19 at 12.)

1. Negligence (First Cause of Action)

To establish negligence, “a plaintiff must prove four elements: (1) a duty requiring the defendant to conform to a certain standard of care; (2) a breach by the defendant of that standard; (3) a causal connection between the defendant’s conduct and the resulting injury; and (4) actual damages.” *Jensen v. EXC, Inc.*, 82 F.4th 835, 857 (9th Cir. 2023) (applying Arizona law); *see also Ileto v. Glock Inc.*, 349 F.3d 1191, 1203 (9th Cir. 2003) (applying the same elements under California law). To establish causation under Arizona law, the plaintiff “must show some reasonable connection between defendant’s act or omission and plaintiff’s damages or injuries.” *Robertson v. Sixpence Inns of Am., Inc.*, 789 P.2d 1040, 1047 (Ariz. 1990); *see also Kirsten v. Calif. Pizza Kitchen, Inc.*, No. 21-CV-09578-DOC-KES, 2022 WL 16894503, at *8 (C.D. Cal. July 29, 2022) (applying California law and requiring a plaintiff to demonstrate actual or legal causation through showing the defendant’s act or omission was a substantial factor in bringing about the injury); *Baton*, 2024 WL 3447511, at *38–39 (same and finding third parties accessing data stolen in a breach was a foreseeable consequent of a failure to take reasonable security measures).

Labor Force first argues that Plaintiffs failed to adequately plead causation, faulting them not providing the relation between their employment and for relying on an unclear timeline. (Doc. 19 at 12–13.) Plaintiffs argue they adequately provided the facts necessary to establish a timeline and support causation at this stage in the litigation. (Doc. 20 at 9.) Labor Force further argues that the dates alone are insufficient to allege causation and posit

1 that “Plaintiffs presuppose this connection is obvious.” (Doc. 21 at 10–11.)

2 The Court is perplexed by how Labor Force conceived that the timeline is anything
3 but conspicuous. The Amended Complaint indicates that both Plaintiffs were employed
4 by Labor Force before the breach occurred and were required to provide their sensitive
5 information as a condition of their employment. (*See* Amended Compl. at 4 ¶¶ 14–16, 6
6 ¶ 26, 7 ¶ 32.) There was a breach of Labor Force’s electronic systems where it stored its
7 employees’ sensitive information and said information was stolen. (*Id.* at 4 ¶ 16, 6 ¶ 26.)
8 Then Plaintiffs, without a notification from Labor Force, discovered that their information
9 was posted on the dark web “with indications that it came from [Labor Force’s] system.”
10 (*Id.* at 4 ¶ 16, 6 ¶ 27.) The Court notes that “indications” is broad, however, construing the
11 timeline with the other allegations discussed previously as true and in context links the
12 events to establish causation of Plaintiffs’ purported injuries. Notably, Plaintiffs allege
13 they took steps to protect their data, dispelling an inference that the information identified
14 on the dark web resulted from some other leak or breach. Plaintiffs also made specific
15 allegations that Labor Force failed to properly implement proper encryption of sensitive
16 information held on its systems. Together, these facts, while they could be more detailed,
17 support a plausible legal theory that Labor Force’s alleged unreasonable security measures
18 and resulting breach caused the injuries, i.e., risk of future fraud or identity theft and
19 mitigation costs. These facts also establish at this stage in the litigation that Labor Force’s
20 alleged unreasonable security measures were a substantial factor that gave rise to the
21 foreseeable threat of fraud or identity theft and mitigation costs associated with such risks.
22 *See, e.g., Baton*, 2024 WL 3447511, at *38–39. Therefore, the Court declines to grant
23 judgment on causation grounds. However, as the Court will explain, Plaintiffs fail to
24 adequately allege cognizable damages to state a valid negligence claim.

25 Next, Labor Force argues that Plaintiff’s claimed damages of “lost time and efforts
26 to mitigate the actual and potential impact of the Data Breach” and the “continued risks of
27 exposure of their Sensitive Information” are speculative and insufficient to establish
28 damages. (Doc. 19 at 13; *see also* Doc. 21 at 11–12.) Plaintiffs argue their claimed

1 damages are sufficient because, in addition to those damages, they also claim damages for
 2 injuries related to the increased risk of fraud and identity theft and expenses for mitigation
 3 efforts are “clearly economic.” (Doc. 20 at 10 (citing Amend Compl. at 7 ¶ 32).)

4 First, regarding the increased risk of fraud and identity theft, Plaintiffs do not allege
 5 that they have actually suffered from fraud or identity theft. Arizona law, however,
 6 requires negligence damages to be more than merely the threat of future harm. *Griffey v.*
 7 *Magellan Health Inc.*, 562 F. Supp. 3d 34, 46 (D. Ariz. 2021) (citing *CDT, Inc. v. Addison,*
 8 *Roberts & Ludwig, C.P.A., P.C.*, 7 P.3d 979, 982–83 (Ariz. Ct. App. 2000)); *see also*
 9 *Quinalty v. FocusIT LLC*, No. CV-23-00207-PHX-JJT, 2024 WL 342454, at *5 (D. Ariz.
 10 Jan. 30, 2024) (finding that threats of imminent and impending injuries from an increased
 11 risk of theft and fraud are not cognizable on their own); *Holly v. Alta Newport Hosp., Inc.*,
 12 612 F. Supp. 3d 1017 (C.D. Cal. 2020) (finding allegations of increased risk of fraud and
 13 identity theft was insufficient to state a negligence claim under California law). Plaintiffs
 14 here assert speculative damages of a future harm that has yet to occur and are not
 15 cognizable.¹

16 Second, regarding mitigation expenses, where out-of-pocket expenses for credit
 17 monitoring are alleged, a plaintiff must also allege the expenses are reasonable and
 18 necessary. *Griffey*, 562 F. Supp. at 47 (noting the reasonableness of expenses involves the
 19 availability of some metric to make that determination); *see also Durgan v. U-Haul Int’l*
 20 *Inc.*, No. CV-22-01565-PHX-MTL, 2023 WL 7114622, at *2 (D. Ariz. Oct. 27, 2023)
 21 (requiring mitigation efforts to be reasonable); *see also Holly*, 612 F. Supp. 3d at 1027
 22 (applying a similar standard under California law). Plaintiffs have not alleged the expenses
 23 are reasonable or necessary, nor have they provided sufficient factual details to gauge the
 24 reasonableness of the expenses related to mitigation efforts.

25 Next, Plaintiffs argue their negligence claim incorporates its damages allegations
 26 for lost time, diminution of value to their sensitive information, and loss of privacy. (Doc.

27 ¹ Plaintiffs cite to *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018) to argue such
 28 damages are sufficient. *Zappos.com*, however, addresses the injury-in-fact inquiry for
 standing purposes, not a failure to state a claim, and Plaintiffs have not explained its
 applicability beyond standing. *See* 888 F.3d at 1028–29.

20 at 9–10 (citing Amend Compl. at 7 ¶ 32).) Lost time is not a cognizable injury for negligence claims. *See Griffey*, 562 F. Supp. 3 at 46; *Medoff v. Minka Lighting, LLC*, No. 2:22-CV-08885-SVW-PVC, 2023 WL 4291973, at *9 (C.D. Cal. May 8, 2023) (“[G]eneralized allegations of lost time and a continued expectation that he will continue bearing these costs are too speculative to constitute a cognizable injury.”); *see also Smallman v. MGM Resorts Int’l*, 638 F. Supp. 3d 1175, 1192 (D. Nev. 2022) (“[T]angible, out-of-pocket expenses are required in order for lost time spent monitoring credit to be cognizable as damages.” (citation omitted)).

For the diminution of value damages, Plaintiffs “must establish both the existence of a market for [their] personal information and an impairment of [their] ability to participate in that market.” *Griffey*, 562 F. Supp. 3 at 46 (quoting *Pruchnicki v. Envision Healthcare Corp. (Pruchnicki I)*, 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), *aff’d*, 845 F. App’x 613 (9th Cir. 2021)). While Plaintiffs allege a criminal market exists for their data, (*see* Amended Compl. at 8–9 ¶ 42), courts have refused to recognize the “dark web” as a legitimate market by which individuals may sell their information. *Id.* Additionally, Plaintiffs have alleged no facts that their sensitive information actually lost value beyond conclusory allegations that the information is valuable to criminals and the breach caused a diminution. *See, e.g., Pruchnicki (Pruchnicki II) v. Envision Healthcare Corp.*, 845 F. App’x 613, 614–15 (9th Cir. 2021). Nor do Plaintiffs allege that they sell their data or any supporting facts to ascertain the value of their data beyond speculation about what it could be sold for on the dark web. *See, e.g., Ruiz v. Gap, Inc.*, 380 F. App’x 689, 691 (9th Cir. 2010) (noting a plaintiff must “establish sufficient appreciable, nonspeculative, present harm to sustain a negligence cause of action under California law”).

Finally, regarding lost privacy damages, Plaintiffs’ allegations seem to relate to their other claims, i.e., invasion of privacy, rather than asserted to establish damages for their negligence claim and have not cited to any authority to support such damages. Therefore, Plaintiffs’ damages theories are not cognizable and insufficient to state a negligence claim. The Court will grant judgment and dismiss the claim.

2. Invasion of Privacy (Second Cause of Action)

Labor Force argues that Plaintiffs fail to state a claim for invasion of privacy because their allegations of intentional conduct are merely conclusory recitals of the elements of the claim. (Doc. 19 at 14.) Plaintiffs in turn argue that their allegations are beyond conclusory and adequately pleaded Labor Force’s conduct was egregious enough to support their claim. (Doc. 20 at 11.)

The parties cite cases addressing invasions of privacy under California law. *See, e.g., S.F. Apartment Ass’n v. City & County of San Francisco*, 881 F.3d 1169, 1178 (9th Cir. 2018); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 16-CV-00014-GPC-BLM, 2016 WL 6523428, at *11–12 (S.D. Cal. Nov. 3, 2016); *Ruiz*, 380 F. App’x at 690; *County of Los Angeles v. Superior Ct.*, 280 Cal. Rptr. 3d 85, 101–02 (Cal. Ct. App. 2021). Those cases generally require a plaintiff to establish: “(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.” *Ruiz*, 380 F. App’x at 690 (quoting *Hill v. Nat’l Collegiate Athletic Assn.*, 865 P.2d 633, 657 (Cal. 1994)) (“Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.” (citation omitted)). “[C]ommon law invasion of privacy by public disclosure of private facts requires that the actionable disclosure be widely published and not confined to a few persons or limited circumstances. *Hill*, 865 P.2d at 648–49.

Courts have rejected finding negligent conduct that leads to the theft of highly personal information, including social security numbers, as establishing actionable conduct under an invasion of privacy claim absent disclosure of medical records. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosing personal data from plaintiffs’ phones to third parties was not an egregious breach of social norms); *Dugas*, 2016 WL 6523428, at *12 (“Plaintiff fails, for example, to allege any facts that would suggest that the data breach was an intentional violation of Plaintiff’s and other class members’ privacy, as opposed to merely a negligent one.”); *County of Los Angeles*, 280

Cal. Rptr. 3d at 106 (relating to medical records); *St. Aubin v. Carbon Health Techs., Inc.*, No. 24-CV-00667-JST, 2024 WL 4369675, at *13 (N.D. Cal. Oct. 1, 2024) (refusing to dismiss an invasion of privacy claim at the motion to dismiss stage where a data breach involved medical information). Plaintiffs' claim relates to their employment records and personal information, notably absent are allegations regarding medical records. As such, mere negligence is insufficient to state a claim. *Dugas*, 2016 WL 6523428, at *11–12; *see generally Steinkamp v. Sw. Airlines, Co.*, No. CV-19-05022-PHX-SPL, 2021 WL 11730573, at *2 (D. Ariz. Mar. 11, 2021) (noting that an invasion of privacy claim under Arizona law requires some intentional act).

Plaintiffs allege that Labor Force acted “with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.” (Amended Compl. at 22 ¶ 101–102.) Plaintiffs purported intentional conduct is based on Labor Force’s inaction, rather than an affirmative act, and appears to be entirely based on negligence. Even if its failure to take proper security precautions was intentional, Labor Force’s dissemination of Plaintiffs’ private information was an unquantified group of hackers in a single breach. Labor Force’s actual disclosure was limited to those hackers and only one alleged instance. There are no allegations that Labor Force intended for third parties to widely disseminate Plaintiffs’ private information. *See Hill*, 865 P.2d at 648–49. Therefore, Plaintiffs have failed to state an invasion of privacy claim.

3. Breach of Implied Contract (Third Cause of Action)

Labor Force argues Plaintiffs’ breach of implied contract claim “fails on causation grounds the same way as [the negligence claim].” (Doc. 19 at 14–15.) Because the Court rejected Labor Force’s causation theory under the negligence claim, Labor Force has failed to show lack of causation here. Therefore, the Court declines to grant judgement on this claim based on the anemic argument.

4. Breach of Fiduciary Duty (Fourth Cause of Action)

Again, Labor Force merely references its ineffective causation argument here and the Court need not repeat it. Therefore, the Court declines to grant judgement on this

1 ground.

2 Labor Force, however, additionally argues no fiduciary relationship exists between
3 it and its employees. (Doc. 19 at 15.) Labor Force cites to cases apply California or
4 Washington law to support its argument. (*See id.* (citing *Wolf v. Superior Ct.*, 130 Cal.
5 Rptr. 2d 860, 866–67 (Cal. Ct. App. 2003) (California law); *In re Premera Blue Cross*
6 *Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1203 (D. Or. 2016) (Washington
7 law).) In response, Plaintiffs, rather than cite to authority establishing an employer owes a
8 fiduciary duty to employees to keep their sensitive information safe, critique Labor Force’s
9 proffered case law as out of state and distinguishable without indicating what law applies.
10 (*Id.* at 12.) Plaintiffs miss the mark.

11 “[I]n the absence of a fiduciary relationship, there can be no breach of fiduciary duty
12 as a matter of law In general, employment-type relationships are not fiduciary
13 relationships.” *Schmidt v. City of Pasadena*, No. LA CV21-08769 JAK (JCX), 2024 WL
14 1640913, at *27 (C.D. Cal. Mar. 21, 2024) (quoting *O’Byrne v. Santa Monica-UCLA Med.*
15 *Ctr.*, 114 Cal. Rptr. 2d 575, 586 (Cal. Ct. App. 2001)). The same is true in Arizona. *See*
16 *Arimilli v. Rezendes*, No. CV-21-00345-PHX-GMS, 2023 WL 2734456, at *3 (D. Ariz.
17 Mar. 31, 2023); *Wilkes v. Elec. Data Sys. Corp.*, No. 04-CV-00341 TUC JMR, 2006 WL
18 753161, at *4 (D. Ariz. Mar. 17, 2006), *aff’d*, 267 F. App’x 661 (9th Cir. 2008); *see also*
19 *See, e.g., Andes Indus., Inc. v. Cheng Sun Lan*, 774 F. App’x 358, 360–61 (9th Cir. 2019)
20 (affirming dismissal of a breach of fiduciary claim where the plaintiff failed to plead facts
21 demonstrating the defendant was in a position of superior power such that the defendant’s
22 will effectively substituted the plaintiffs). Plaintiffs base their claim on a legal theory that
23 a fiduciary duty exists under a special relationship in which they entrusted their sensitive
24 information to Labor Force as part of their employment. (Amended Compl. at 24–25
25 ¶¶ 116–120.) Plaintiffs’ claim here relies on mere conclusory allegations that a fiduciary
26 duty exists and failed to provide any legal support such a duty exists under these
27 circumstances. This is insufficient to state a claim. Therefore, the Court will grant
28 judgment on this claim.

1 5. Breach of Confidence (Fifth Cause of Action)

2 To establish a claim for breach of confidence under California law, a plaintiff must
3 demonstrate that: “(1) the plaintiff conveyed ‘confidential and novel information’ to the
4 defendant; (2) the defendant had knowledge that the information was being disclosed in
5 confidence; (3) there was an understanding between the defendant and the plaintiff that the
6 confidence be maintained; and (4) there was a disclosure or use in violation of the
7 understanding.” *Ent. Rsch. Grp., Inc. v. Genesis Creative Grp., Inc.*, 122 F.3d 1211, 1227
8 (9th Cir. 1997). California courts have held that this disclosure requires the defendant to
9 affirmatively share the information with a third party. *In re Ambry Genetics Data Breach*
10 *Litig.*, 567 F. Supp. 3d 1130, 1146–47 (C.D. Cal. 2021) (finding a breach of confidence
11 claim failed where the plaintiff alleged a third party stole the information, not that the
12 defendant affirmatively shared such information).

13 Labor Force, citing the cases above, argues Plaintiffs fail to allege that it voluntarily
14 disclosed the sensitive information. (Doc. 19 at 15–16.) Plaintiffs respond, arguing that
15 Labor Force voluntarily chose not to notify them of the breach, and as such, this fact
16 adequately supports the claim. (Doc. 20 at 12–13.) Again, rather than provide any law to
17 support its legal theory, Plaintiffs fail to refute that they do not allege Labor Force
18 affirmatively shared any information with third parties. In disregard of this requirement,
19 Plaintiffs incorrectly posit that inaction after a third party stole the information supports
20 such a claim without any legal support. Accordingly, Plaintiffs fail to state breach of
21 confidence claim and thus the Court will grant judgment on this claim.

22 6. Violation of the California Unfair Competition Law (Sixth Cause of
23 Action)

24 The UCL’s coverage is broad, defining “unfair competition” to include “any
25 unlawful, unfair or fraudulent business act or practice.” *Cel-Tech Commc’ns, Inc. v. Los*
26 *Angeles Cellular Tel. Co.*, 973 P.2d 527, 539 (Cal. 1999) (citing Cal. Bus. & Prof. Code
27 § 17200). “Its coverage is sweeping, embracing anything that can properly be called a
28 business practice and that at the same time is forbidden by law.” *Id.* (cleaned up)

(explaining § 17200 borrows violations from other laws and treats them as independently actionable unlawful practices, but a practice “may be deemed unfair even if not specifically proscribed by some other law”). The UCL “is violated where a defendant’s act or practice is (1) unlawful, (2) unfair, (3) fraudulent, or (4) in violation of section 17500 (false or misleading advertisements).” *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). The UCL is not an all-purpose substitute for a tort or contract action.” *Cortez v. Purolator Air Filtration Prods. Co.*, 999 P.2d 706, 712 (Cal. 2000).

Plaintiffs clarify that they assert their UCL claim under the unlawful and unfair prongs. (*See* Doc. 20 at 13.) Plaintiffs allege that Labor Force engaged in unlawful and unfair acts and practices by (1) establishing sub-standard security practices; (2) soliciting and collecting Plaintiffs’ and the Class’s sensitive information know it was not adequately protected; (3) storing the information on an unreasonably unsecure system in violation of California Civil Code § 1798.81.5; and (4) failing to disclose the breach in a timely manner in violation of California Civil Code § 1798.82. (Amended Compl. at 28 ¶¶ 134–135.) Labor Force argues that Plaintiffs failed to show violations of the unfairness prong under the application test and unlawful prong for the same reasons Plaintiffs failed to state a claim for those statutory violations. (Doc. 19 at 16–17.) Plaintiffs respond that their alleged statutory violations support their claim, and their unfairness allegations are adequate. (Doc. 20 at 14.) Labor Force replies maintaining that the unfairness allegations are insufficient and further asserts former employees lack standing to seek injunctive relief against their former employer. (Doc. 21 at 14–15.)

The Court first addresses the standing issue. “[A] plaintiff must establish standing separately for each form of relief sought.” *Friends of the Earth, Inc. v. Laidlaw Env’t Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000); *see also Davis v. Fed. Election Comm’n*, 554 U.S. 724, 734 (2008). Standing under the UCL requires plaintiffs to demonstrate they “lost money or property” that occurred “as a result of unfair competition.” *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 965 (S.D. Cal. 2012); *Kwikset Corp. v. Superior Ct.*, 246 P.3d 877, 885–84 (Cal. 2011); Cal. Bus. & Prof. Code

§ 17204. For a plaintiff to establish he has “lost money or property,” the plaintiff “must demonstrate some form of economic injury,” which may include entering “into a transaction, costing money or property, that would otherwise have been unnecessary.” *Kwikset*, 246 P.3d at 885–86.

Plaintiffs advance that they “lost money and property,” apparently in the form of costs associated with protecting themselves from the consequences of the breach. (*See* Amended Compl. at 3 ¶ 9, 11–12 ¶ 61, 29 ¶ 137.) To the extent Plaintiffs allege other injuries, they are inapplicable. *See, e.g., In re Sony Gaming Networks*, 903 F. Supp. 2d at 966 (“Plaintiffs’ allegations that the heightened risk of identity theft, time . . . spent on mitigation of that risk, and property value in one’s information, do not suffice as injury under the UCL.”); *see also In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) (“Numerous courts have held that a plaintiff’s “personal information” does not constitute money or property under the UCL.”). But courts have disagreed whether mitigation expenses suffice under the UCL. *Compare id.* (finding money spent on mitigation of the risk insufficient), *with Corona v. Sony Pictures Ent., Inc.*, No. 14-CV-09600-RGK-EX, 2015 WL 3916744, at *8 (C.D. Cal. June 15, 2015) (finding mitigation expenses were a valid economic loss). Where mitigation costs were sufficient, the court found that they were also reasonable and necessary. *See Corona*, 2015 WL 3916744, at *4–5, 8. As noted, Plaintiffs have failed to allege their costs were both reasonable and necessary. Therefore, Plaintiffs have insufficiently pleaded they lost money or property to establish standing and state a claim under the UCL.²

///

² Assuming their mitigation costs do confer sufficient standing, even if Plaintiffs were to prevail, injunctive relief remains the only possible remedy under the claim. *See, e.g., Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242, at *8 (N.D. Cal. Sept. 14, 2016) (dismissing a UCL data breach claim where plaintiffs failed to allege the defendant derived a benefit to entitle them to restitution and failed to allege nonspeculative future harm to support entitlement to injunctive relief). Any connection between monies paid to mitigate and respond to the breach would relate to damages and are not available under the UCL. *Smith v. Antioch Unified Sch. Dist.*, No. 16-CV-01676-RS, 2016 WL 5419434, at *4 (N.D. Cal. Sept. 26, 2016) (“A restitution order against a defendant thus requires both that money or property have been lost by a plaintiff, on the one hand, and that it have been acquired by a defendant, on the other.”).

1 7. Violation of the California Customer Records Act (Cause of Action
 2 Seven)

3 Plaintiffs allege that Labor Force violated the CRA by failing to notify them of the
 4 breach entirely, let alone within a reasonable time. (Amended Compl. at 29–32
 5 ¶¶ 140–151.) Labor Force argues that Plaintiffs fail to state a claim because they simply
 6 recite the elements of the applicable statute without explanation. (Doc. 19 at 17, Doc. 21
 7 at 15–16.) Plaintiffs respond that they adequately plead the claim, arguing Labor Force’s
 8 argument lacks merit. (Doc. 20 at 14–15.)

9 The CRA regulates businesses’ treatment and notification procedures relating to its
 10 customers’ personal information. *See* Cal. Civ. Code §§ 1798.80 to .85. The CRA
 11 “protect[s] California residents in their role [as] customers.” *Corona*, 2015 WL 3916744,
 12 at *7; *see also Kirsten*, 2022 WL 16894503, at *6 (finding the CRA was inapplicable to
 13 information provided to an employer as a condition of employment). Plaintiffs do not
 14 allege that they are customers—they are employees who provided their information
 15 allegedly as a condition of employment. (Amended Compl. at 7 ¶ 32.) Therefore, the CRA
 16 does not apply under these facts and Plaintiffs fail to state such a claim.

17 8. Violation of the California Consumer Privacy Act (Cause of Action
 18 Eight)

19 Labor Force once again relies on their faulty causation argument for this claim and
 20 reduces its briefing to two short paragraphs essentially make conclusory argument that
 21 Plaintiffs merely recite the elements of the claim. (Doc. 19 at 17.) The CPA provides:
 22 “Any consumer whose . . . personal information . . . is subject to an unauthorized access
 23 and exfiltration, theft, or disclosure as a result of [a] business’s violation of the duty to
 24 implement and maintain reasonable security procedures and practices appropriate to the
 25 nature of the information to protect the personal information may institute a civil action.”
 26 Cal. Civ. Code § 1798.150(A). As previously discussed, Plaintiffs allege that Labor Force
 27 failed to comply with industry standards, and specifically the proper encryption of PII,
 28 training employees on how to protect PII, and correct software and network configurations.

1 Such allegations are sufficient at this stage in the litigation and go to the reasonableness of
2 Labor Force's security measures. *See, e.g., Kirsten*, 2022 WL 16894503, at *3 (allowing
3 unauthorized access to protected information online was sufficient to state a claim). Thus,
4 the Court declines to grant judgment on this claim.

5 **C. Leave to Amend**

6 Federal Rule of Civil Procedure 15(a) requires that leave to amend be "freely give[n]
7 when justice so requires." Leave to amend should not be denied unless "the proposed
8 amendment either lacks merit or would not serve any purpose because to grant it would be
9 futile in saving the plaintiff's suit." *Universal Mortg. Co. v. Prudential Ins. Co.*, 799 F.2d
10 458, 459 (9th Cir. 1986). Therefore, "a district court should grant leave to amend even if
11 no request to amend the pleading was made, unless it determines that the pleading could
12 not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122,
13 1127 (9th Cir. 2000) (cleaned up).

14 While Plaintiffs have not requested leave to amend, Labor Force has not argued that
15 it would be prejudiced if Plaintiffs amend their claims. Because Plaintiffs have failed to
16 state a claim under Causes of Action One, Two, Four, Five, Six, and Seven and Plaintiffs
17 could remedy the deficiencies identified, albeit how Plaintiffs may cure those deficiencies
18 is not abundantly clear to the Court. It is inappropriate for the Court to dismiss the claims
19 with prejudice at this time. Thus, the Court will grant leave to amend those causes of
20 action, albeit, how Plaintiffs may cure those deficiencies is not abundantly clear to the
21 Court.

22 **IV. CONCLUSION**

23 Accordingly,


24 **IT IS HEREBY ORDERED granting in part** Labor Force's Motion for
25 Judgement on the Pleadings (Doc. 19) in part with respect to Causes of Action One, Two,
26 Four, Five, Six, and Seven, and **denying in part** otherwise.

27 **IT IS FURTHER ORDERED dismissing** the following claims in Plaintiffs'
28 Amended Complaint (Doc. 16): Negligence; Invasion of Privacy; Breach of Fiduciary

1 Duty; Breach of Confidence; Violation of the California Unfair Competition Law; and
2 Violation of the California Customer Records Act without prejudice.

3 **IT IS FURTHER ORDERED** granting Plaintiffs leave to amend and that
4 Plaintiffs shall file a Second Amended Complaint, if they so choose, **no later than 30 days**
5 **after this Order is filed.**

6 Dated this 22nd day of January, 2025.

7
8 
9 _____
Honorable Susan M. Brnovich
United States District Judge